Statement of
MG Robert T. Howard (Ret)
Senior Advisor to the Deputy Secretary
Supervisor, Office of Information and Technology

Before the
U.S. House of Representatives
Committee on Veterans' Affairs

June 28, 2006

Mr. Chairman and members of the Committee, good morning. Thank you for your invitation to discuss the Department of Veterans Affairs information technology reorganization plan and the recent data loss incident.
I am accompanied today by Mr. Joseph K. Shaffer, Director, VA IT System Model Realignment Office and Mr. Pedro Cadenas, Jr. Associate Deputy Assistant Secretary for Cyber and Information Security. I request that my written testimony be entered into the record.

I would first like to give you an update on the VA IT realignment. The VA IT System Model has been developed and approved. The two principal underpinnings of the VA IT realignment are to ensure: (1) continued world-class service to our veterans, and (2) our continued commitment to patient safety.

The key area of focus is to transition VA's IT community to operate within the VA IT Management System that separates the Development and Operations and Maintenance domains. Hence, VA will establish required business practices and processes that harmonize the oversight and budgetary responsibilities of the Office of the CIO, the functionality of the Domains, and business relationships of the IT service provider and the customer for all IT activities across the entire VA.

As background, in an Executive Decision Memorandum dated October 19, 2005, the Secretary of the Department of Veterans Affairs (Secretary) approved the concept of a new IT Management System for the VA. This decision to move to the VA IT Management System was made to correct longstanding deficiencies in the current decentralized IT management system. The concept of a new VA IT Management System initially separates the IT community into two domains – an *Operation and Maintenance (O&M) Domain* that is the responsibility of the Assistant Secretary for Information Technology (AS/IT) / (VA CIO) and a much smaller *Application Development Domain* that is the responsibility of the Administrations and Staff Offices. Although the domains are separated, the VA CIO retains oversight responsibilities for all VA IT projects. As Secretary Nicholson testified at the House Appropriations Committee hearing on June 27, 2006, the long-range plan is to bring the Application Development Domain into the larger O&M domain resulting in a single domain for IT.

To achieve greater clarity and understanding of the design and processes of the VA IT Management System, the Secretary directed the development of a Model that would be used to guide the development of a more thorough IT Transition and Implementation Plan. As noted above, the goal is for the Department of Veterans Affairs to complete the transition to this new VA IT Management System on or about July, 2008.

The VA IT System Model will strengthen the protection of all sensitive information As VA's General Counsel Tim McClain testified last week, the Federal Information Security Management Act (FISMA) requires the Secretary to delegate to the CIO sufficient authority to "ensure compliance" by the agency with the above information-security requirements. This must include the authority to (1) create and operate the agency-wide information security program; (2) establish information security policies and procedures and control techniques for the agency, which, when followed, will ensure compliance with all of the above requirements; (3) train and oversee personnel with significant responsibilities for information security; and (4) assist senior agency officials concerning their information security responsibilities, including the analysis process.

The agency-wide security program directed by FISMA should provide systematic guidance for the conduct of the risk analysis process, security awareness training for all VA personnel, periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, a process for remedial action, procedures for detecting security incidents, and plans for ensuring continuity of operations for information systems. The policies and procedures should interpret, explain, and apply to VA the applicable external standards and provide guidance for the application of these standards to VA operations. The control techniques should permit monitoring of the numerous activities in which programs are required to engage to determine that they are accomplished in accordance with applicable standards and that any appropriate remedial actions are timely undertaken. The program, policies, procedures, and control techniques, and any other actions, should be developed in mutual coordination, cooperation, and collaboration between the CIO and program officials.

FISMA does not necessarily require delegation to the CIO of direct control over agency programs, because such control is not the only means by which the information security-objectives may be accomplished. For example, even without direct control over certain programs, a CIO could endeavor to ensure compliance with governing standards through training and otherwise influencing the behaviors of key program-security personnel. While an agency head certainly may choose to confer certain enforcement powers on the CIO, e.g., the ability to sanction program officials outside the CIO's immediate organization for noncompliance with departmental policies, we do not read FISMA to require it.

The VA IT System Model was developed as a framework for VA's future IT Management System. The principal elements of this *IT System Model* include:

1. Definitions of the roles, responsibilities and initial boundaries between the *Operations and Maintenance (O&M) Domain* that is the responsibility of the AS/IT (CIO) and an *Application Development Domain*, to include determination of business needs and priorities that is the responsibility of the Administrations and Staff Offices. Although the Domains are separated, the Model sets forth essential cohesion between the domains in order to provide the CIO with oversight and budget responsibilities for all VA IT projects.
2. Authority, delegation of authority, and governance structure and process for the conduct of all VA IT-related business;
3. Key IT service delivery business process flows;
4. Sample scenarios to illustrate how Domain activities are coordinated by process flows. These process flows must be clearly defined to reflect the critical interdependence of business applications and the performance of the IT infrastructure; and
5. A recommended "To-Be" organization for the office of the CIO designed to balance the tactical needs of operating a complex infrastructure as a shared service with the strategic needs of aligning IT resources to best meet the mission requirements of the Department.

As you are aware, the Secretary initiated several recent actions to tighten our privacy and data security programs. On May 24 the "Data Security-Assessment and Strengthening of Controls" program was established to provide a high priority and much more focused effort to strengthen our data privacy and security procedures. The two principal objectives of this program are to first, reduce the risk of a recurrence of incidents such as the recent data los, and second, to remedy the material weakness reported by the Inspector General. There are three phases to this effort; Assessment, Strengthening of Controls, and Enforcement. We are almost through the Assessment Phase and have actions underway in the other two phases as well.

On May 26 the Secretary issued a Directive that requires the top leadership to instruct all VA managers, supervisors, and team leaders of their duty and responsibility to protect sensitive and confidential information. In this memo the Secretary also announced that he had convened a task force of VA senior leaders to review all aspects of information security and make recommendations to strengthen our protection of sensitive information. One of the first tasks of this group is to complete an inventory of all positions requiring access to sensitive VA data by June 30.

We began a Security Awareness Week at all VA facilities (hospitals, clinics, regional offices, and cemeteries) on Monday June 26. Each day managers are expected to focus on one or more elements of information security in meetings.

We are emphasizing training in privacy and cyber security for all employees. We require all VA employees, contractors, and volunteers to complete both Cyber Security and Privacy Training, annually. Both designed to help VA employees understand the importance of protecting sensitive information and make them aware of their responsibilities to protect this information. Normally, employees are required to complete this training by September 30 of each year. However, given the recent incident, the Secretary has directed all employees to complete both courses by June 30.

We will be conducting a Department-wide inventory of laptops to ensure that they carry the encryption and other cyber security software necessary to ensure remote access users are operating in a safe and secure environment.

This effort is on hold, however, due to a recent lawsuit. It will continue once legal clearance is obtained.

Finally, we are reviewing all policies, directives, and handbooks relating to privacy, cyber security and records management to ensure they are accurate, clear and focused.

These efforts will provide for a more secure environment for sensitive data used in VA. Mr. Chairman, that concludes my statement. Thank you for the opportunity to appear before you today.